REMARKS / ARGUMENTS

Claims 1-12 and 14-15 remain pending in this application. Claim 13 has been canceled without prejudice or disclaimer. No new claims have been added.

Priority

Applicants appreciate the Examiner's acknowledgment of the claim for priority and safe receipt of the priority document.

Claim Objections

Claim 1 has been amended to overcome the Examiner's objection.

35 U.S.C. §112

Claim 10 has been amended to overcome the Examiner's rejection under this section. The Examiner is hereby invited to contact the undersigned by telephone if any further changes are deemed necessary.

35 U.S.C. §103

Claims 1-2, 4-9 and 13-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Davis (U.S. Patent No. 5,805,712) in view of Yepez, III et al (U.S. Patent No. 5,535,168). Claim 3 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Yepez, III et al in further view of Hartman (U.S.

Patent No. 5,224,166). Claim 15 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Davis in view of Yepez, III et al in further view of Nagai (U.S. Patent No. 6,571,263). These rejections are traversed as follows.

The present invention is directed to an information processing apparatus, as recited in claim 1, having a processing device and a bus for interconnecting the processing device and other component devices. The processing device is integrated on a single semiconductor chip and internally generates key information and encrypts sensitive information inputted from the bus with generated key information. The processing device outputs the encrypted sensitive information to the bus without outputting the key information. Furthermore, the processing device newly generates key information each time sensitive information inputted from the bus is encrypted. This last feature was recited in claim 13 and has now been incorporated into claims 1 and 10. Claim 13 has been canceled. Claim 10 was not rejected over prior art and recites this feature using different language. Nonetheless, the arguments made herein with respect to claim 1 should apply to claim 10.

None of the cited references, whether taken individually or in combination, recites these features of the presently claimed invention. For example, Davis discloses a semiconductor device for storing encryption/decryption keys upon manufacture in combination with digital certificates. The semiconductor device includes a non-volatile memory capable of storing the encryption/decryption keys and at least one digital certificate, an internal memory capable of temporarily storing information input into the semiconductor device from another device and possibly

encryption and decryption algorithms, a processor for processing the information, and a random number generator for generating the encryption/decryption keys internally to the semiconductor device.

However, as mentioned above, according to the present invention, the processing device newly generates key information each time sensitive information inputted from the bus is encrypted, as recited in claim 1. Therefore, the present invention has the advantage that since key information is different for each sensitive information to be encrypted, all of the encrypted sensitive information is not deciphered even if some encrypted sensitive information is deciphered.

In rejecting claim 13, the Examiner states that Davis discloses this feature at column 5, lines 46-64. However, this portion of Davis only discloses steps for manufacturing the hardware agent (see column 5, lines 35 to column 6, line 7) and does not disclose that information inputted from an external device is encrypted. In other words, Davis merely discloses that a hardware agent generates another public/private key pair only if the public key that is generated and outputted by the hardware agent is identical to a previously generated public key that is stored in the storage device of the certification system, such that the public/private key pair is unique. However, Davis does not disclose that the hardware agent generates the public/private key pair each time information inputted from an external device is encrypted. Therefore, it is submitted that the Examiner's rejection cannot be maintained.

Davis discloses steps for remote verification of the hardware agent (see column 6, lines 8-41). However, Davis merely discloses that the hardware agent encrypts a "random challenge" (i.e., a data sequence for testing purposes) that is generated and transmitted by the remote system with the private key of the public/private key pair that has already been generated in the steps of manufacturing the hardware agent. Davis does not disclose that the hardware agent newly generates the private key each time the random challenge is encrypted. Therefore, Davis clearly fails to disclose a feature of the present invention directed to the processing device newly generating key information each time sensitive information inputted from the bus is encrypted as recited in claim 1.

The deficiencies in Davis are not overcome by resort to Yepez, III et al. Yepez, III et al discloses a flow diagram in Fig. 3 illustrating that an alarm detector monitors (step 310) the environment for triggering events such as opening a housing containing a device, operating the device at extremely high or extremely low temperatures, operating the device at excessive voltage levels or even an external "erase memory" command. When an alarm is detected and the memory has not been erased, the memory is erased (step 320) using nonerasure techniques, such as a processor writing information to memory (see column 4, lines 13-36). Therefore, Yepez, III et al discloses that information in a memory is deleted if an abnormality is detected. However, Yepez, III et al does not disclose that the processing device newly generates key information each time sensitive information inputted from the bus is encrypted, as recited in claim 1.

The deficiencies in Davis and Yepez, III et al are not overcome by resort to Hartman nor Nagai. Neither of these references disclose that the processing device newly generates key information each time sensitive information inputted from the bus is encrypted.

Conclusion

In view of the foregoing, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

By_____
Shrinath Malur
Reg. No. 34,663
(703) 684-1120